10

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/058,689 | 01/28/2002 | David Aro Bruton III | RSW920020011US1 | 4064 |

7590 01/13/2006

Jerry W. Henrndon
IBM Corporation T81/503
PO Box 12195
Research Triangle Park, NC 27709

| EXAMINER | |
|---|---|
| DAVIS, ZACHARY A | |
| ART UNIT | PAPER NUMBER |
| 2137 | |

DATE MAILED: 01/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| | | | |
|---|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>10/058,689 | **Applicant(s)**<br>BRUTON ET AL. | |
| | **Examiner**<br>Zachary A. Davis | **Art Unit**<br>2137 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *18 October 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-44* is/are pending in the application.

4a) Of the above claim(s) *16-21,28-31 and 41-44* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15,22-27 and 32-40* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *20020128*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

## DETAILED ACTION

### *Election/Restrictions*

1. Applicant's election without traverse of Species A, Claims 1-15, 22-27, and 32-40 in the reply filed on 18 October 2005 is acknowledged.

2. Claims 16-21, 28-31, and 41-44 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected species, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on 18 October 2005.

### *Specification*

3. The disclosure is objected to because of the following informalities:

The first paragraph of the specification includes blank spaces left for application and/or patent numbers of related applications. These must be updated to include all current application numbers, and the status of the applications if issued or abandoned.

Appropriate correction is required.

4. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the

specification. The Examiner recommends particular attention to ensure that all reference numerals referring to the drawing figures are correct.

## *Claim Objections*

5. Claim 37 is objected to because of the following informalities: Claim 37 recites "The computer program product according to Claim 1"; however, Claim 1 is directed to a method. It appears that Claim 37 is instead intended to depend from Claim 32. Appropriate correction is required.

## *Claim Rejections - 35 USC § 112*

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claim 8 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 8 recites the limitation "the intrusion detection policy information". There is insufficient antecedent basis for this limitation in the claims.

### *Claim Rejections - 35 USC § 102*

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1-15, 22-27, and 32-40 are rejected under 35 U.S.C. 102(e) as being anticipated by Vaidya, US Patent 6279113.

In reference to Claims 1 and 2, Vaidya discloses a method of intrusion detection in a network, where intrusion suspicion levels are defined for inbound communications, defining a sensitivity level for filtering intrusion events, determining a suspicion level for a particular inbound communication, and determining if the particular inbound communication should be treated as an intrusion event by comparing the sensitivity level to the determined suspicion level (see column 7, line 52-column 8, line 39, noting that higher sensitivity to certain actions with different levels of suspicion, depending on the previous conditions met in a "sequential" profile, or on the timing and count values in a "timer/counter" profile, will make detection of an attack more likely; for example, if a first condition has been met in a sequential profile, column 7, lines 52-67, then the sensitivity level is raised for the next packets, and if those packets have an appropriate suspicion level, column 8 lines 1-15, then an intrusion event is detected).

In reference to Claims 3 and 4, Vaidya further discloses comparing conditions in the computing device, specifically contents of the particular inbound communication, to predetermined conditions signaling a potential intrusion (column 5, lines 27-33).

In reference to Claim 5, Vaidya further discloses that conditions can include the state of a protocol stack (column 7, lines 18-24; column 8, lines 40-56).

In reference to Claims 6-8, Vaidya further discloses taking defensive actions when it is determined that the inbound communication should be treated as an intrusion, where the defensive actions are determined from policy information stored in a repository (column 6, lines 18-26; column 5, lines 27-33).

In reference to Claims 9 and 10, Vaidya further discloses comparing the inbound communication to an attack signature, where a signature can represent a class of attacks (column 6, lines 27-40).

In reference to Claim 11, Vaidya further discloses the signatures as conditions to be fulfilled in detection rules, where the rules also include actions to be taken in response to detection of an intrusion event (column 5, lines 33-39; column 6, lines 18-26).

In reference to Claims 12 and 13, Vaidya further discloses operation within layer-specific logic in a protocol stack (column 7, lines 18-26).

In reference to Claim 14, Vaidya further discloses operation in a network analysis device (column 5, lines 18-26).

In reference to Claim 15, Vaidya further discloses defining conditions for a plurality of potential intrusion events, associating sensitivity levels with the conditions, determining a suspicion level for the inbound communication, and determining if the conditions of the inbound communication match the selected conditions and the suspicion level maps to the selected sensitivity level (see column 7, line 52-column 8, line 39, noting that higher sensitivity to certain actions with different levels of suspicion, depending on the previous conditions met in a "sequential" profile, or on the timing and count values in a "timer/counter" profile, will make detection of an attack more likely; note also column 5, lines 27-33 where a plurality of profiles are defined).

Claims 22-27 are directed to a system and recite limitations corresponding to those recited in Claims 1-3, 6, 7, 9, 11, and 15, and are rejected by a similar rationale.

Claims 32-40 are directed to a software implementation and recite limitations corresponding to those recited in Claims 1-7, 9, 10, 12, 14, and 15, and are rejected by a similar rationale.

## *Conclusion*

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Porras et al, US Patent 6321338, discloses a statistical intrusion-detection system in which events can have varying levels of suspicion assigned.

b. Magdych et al, US Patent 6546493, discloses an intrusion detection system that includes analysis of attack signatures, and in which the desired sensitivity can be set.

c. Campbell et al, US Patent 6839850, discloses an intrusion detection system that can include sensitivity levels.

d. Holland, III et al, US Patent 6851061, discloses an intrusion detection system that analyzes traffic at various layers in the protocol stack.

e. Ko, US Patent 6983380, discloses an intrusion detection system in which generic attack signatures can be defined.

f. Valdes et al, US Patent Application Publication 2002/0059078, discloses a probabilistic intrusion-detection system in which events can have various levels of suspicion and sensitivity assigned, and where events and alerts are correlated by similarity. .

g. Tsafnat et al, US Patent Application Publication 2003/0061513, discloses a system for detecting denial-of-service attacks that monitors activity profiles within the protocol stack in the kernel.

h. Tarquini et al, US Patent Application Publication 2003/0084319, discloses an intrusion prevention system to be inserted in the network protocol stack.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-

3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

zad

E. Moise
**EMMANUEL L. MOISE**
**SUPERVISORY PATENT EXAMINER**